IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

SUSAN ROMAN, individually and on behalf of all others similarly situated, *Plaintiff,* *v.* COMMUNITY HEALTH SYSTEMS, INC., a Delaware corporation, and COMMUNITY HEALTH SYSTEMS PROFESSIONAL SERVICES CORPORATION, a Delaware corporation, *Defendants.*	Case No.: Complaint--Class Action

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Susan Roman brings this Class Action Complaint and Demand for Jury Trial against Defendants Community Health Systems, Inc. and Community Health Systems Professional Services Corporation (collectively referred to in the singular as "Community Health") and alleges as follows upon personal knowledge as to herself and her own acts and experiences, and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against Community Health for its failure to protect its patients' confidential sensitive information—including their

protected health information as defined by the Health Insurance Portability and Accountability Act ("HIPAA"), Social Security numbers, full names, addresses, dates of birth, and telephone numbers (collectively, "Sensitive Information").

2. Community Health is one of the largest hospital organizations in the country, with over 206 facilities in 29 states.

3. As a health care provider, Community Health is required to protect its patients' Sensitive Information by adopting and implementing the specific data security regulations and standards set forth under HIPAA.

4. In addition to its implied statutory obligation, Community Health expressly promises—through its privacy policies and patient agreements—to safeguard and protect the confidentiality of its patients' Sensitive Information in accordance with HIPAA regulations and industry standards.

5. Unfortunately, it took a massive medical data breach (the largest of its type, in fact) to reveal—for the first time—that Community Health failed to provide its patients' with the level of data protection that they were promised and for which they paid for.

6. Indeed, in July 2014, Community Health confirmed that its computer network had been breached and that the Sensitive Information of approximately 4.5 millions of its patients—including their names, addresses, telephone numbers,

dates of birth, and Social Security numbers—was compromised.

7. Early reports suggest that third parties were able to gain access to Community Health's network—and the highly Sensitive Information it contained—by exploiting a widely-known vulnerability in their server's encryption software, commonly referred to as the "Heartbleed bug." As discussed more fully below, the Heartbleed bug essentially allows anyone on the Internet to access vulnerable servers (like Community Health's) and to, in turn, steal data directly from them. Unfortunately, Community Health didn't fix this well-publicized vulnerability (despite readily available solutions), nor did it implement adequate protections to detect and remove other security threats, which resulted in this massive data breach.

8. By maintaining its patients' Sensitive Information in electronic databases that lacked crucial security measures and industry standard data protections, Community Health jeopardized millions of its patients' Sensitive Information and broke the paid-for promises and contractual obligations that it made to its patients through its patient agreements and privacy policies.

9. Unfortunately, as a result of Community Health's failure to implement and follow these basic security procedures, Plaintiff's and the Class's Sensitive Information is now in the hands of unknown third parties.

PARTIES

10. Plaintiff Susan Roman is a natural person and citizen of the Commonwealth of Pennsylvania.

11. Defendant Community Health Systems, Inc. is a corporation existing under the laws of the State of Delaware with its principal place of business located at 4000 Meridian Boulevard, Franklin, Tennessee 37067. Defendant Community Health Systems, Inc. is also registered to conduct business in the Commonwealth of Pennsylvania. Defendant Community Health Systems, Inc. conducts business throughout this District, the Commonwealth of Pennsylvania, and the United States.

12. Defendant Community Health Systems Professional Services Corporation is a corporation existing under the laws of the State of Delaware with its principal place of business located at 4000 Meridian Boulevard, Franklin, Tennessee 37067. Defendant Community Health Systems Professional Services Corporation is also registered to conduct business in the Commonwealth of Pennsylvania. Defendant Community Health Systems Professional Services Corporation conducts business throughout this District, the Commonwealth of Pennsylvania, and the United States.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2) because (a) at least one member of the putative Class is a citizen of a state different from Defendants, (b) the amount in controversy exceeds $5,000,000 exclusive of interest and costs, and (c) none of the exceptions under that subsection apply to this action.

14. This Court has personal jurisdiction over Defendants because they are registered to conduct business in Pennsylvania, regularly conduct business in Pennsylvania, have hospitals and other offices located in Pennsylvania, and the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from Pennsylvania.

15. Venue is proper pursuant to 28 U.S.C. § 1391(b) because Defendants reside in this District, and because the unlawful conduct alleged in the Complaint occurred in, was directed to, and/or emanated, in part, from Pennsylvania. Venue is additionally proper because Defendants maintain hospitals and other administrative offices in this District.

FACTUAL BACKGROUND

Community Health's Privacy Policies and Patient Agreements Promised to Keep Patients' Sensitive Information Confidential

16. Through its Notice of Privacy Practices (which all patients receive

upon admission to its hospitals and facilities), Community Health represented that it would protect its patients' Sensitive Information and keep it confidential. For instance, the Notice of Privacy Practices stated in relevant part:

> "We understand that medical information about you and your healthcare is personal. We are committed to protecting medical information about you. A record is created of the care and services you receive at this facility. This record is needed to provide the necessary care and to comply with legal requirements."[1]
>
> * * *
>
> "This notice applies to all of the records of your care generated by the facility . . . This notice will tell about the ways in which the facility may use and disclose medical information about you. Also described are your rights and certain obligations we have regarding the use and disclosure of medical information. The law requires the facility to: [m]ake sure that medical information that identifies you is kept private; [i]nform you of our legal duties and privacy practices with respect to medical information about you; and [f]ollow the terms of the notice that is currently in effect . . . ."[2]

17. Similarly, in its "Code of Conduct", Community Health asserts the following:

> "When a patient enters a CHS affiliated facility, a large amount of personal, medical, and insurance data is collected and used to satisfy information needs including the ability to make decisions about a patient's care. We consider patient information highly confidential . . . ."[3]

---

1 *See Community Health's Notice of Privacy Practices*, http://webapps.chs.net/HIPAA/ (last visited Aug. 26, 2014).

2 *Id.*

3 *See Community Health Systems Code of Conduct 2014*, http://www.chs.net/wp-

* * *

> "We are dedicated to compliance with all federal, state, and local laws, rules, and regulations, including privacy and security of patient health information . . . ."[4]

18. Community Health reiterated its obligations to protect its patients' Sensitive Information through many of its affiliate hospitals' "Patient Rights and Responsibilities" agreements, which stated that patients had the right to have their "records related to care . . . to be treated as private."[5]

19. Community Health's statements about its data security and management practices—both through its privacy policies and public representations—served to falsely inflate the advertised utility of its services, thus allowing it and/or its affiliates to charge patients higher costs for treatment.

The Data Breach Revealed for the First Time That Community Health Failed to Properly Protect its Patients' Sensitive Information

20. In July 2014, Community Health confirmed that its computer network was the target of an "external, criminal cyber attack that [it] believes occurred in

---

content/uploads/PDF/2014%20Code%20of%20Conduct.pdf (last visited Aug. 26, 2014).

4 *Id.*

5 *See, e.g.*, Patient Rights and Responsibilities, http://www.mth.org.c1.previewmysite.com/patients-and-visitors/patients-rights/ (last visited Aug. 26, 2014).

April and June, 2014."[6] Community Health's database(s) contained the Sensitive Information of over 4.5 million of its patients, including Plaintiff's and putative Class members'.[7]

21. On August 18, 2014, *nearly five months after the breach*, Community Health Systems, Inc. filed a document with the United States Securities and Exchange Commission detailing the results of its preliminary investigation into the breach.[8]

22. In that document, Community Health also represented that it would be providing appropriate notification to affected patients and regulatory agencies as required by federal and state law. As of the date of filing this Complaint, however, Community Health has not mailed letters or otherwise contacted affected individuals whose Sensitive Information was compromised to inform them of the breach.

---

6 Community Health Systems, Inc.'s Form 8-K, http://www.sec.gov/Archives/edgar/data/1108109/000119312514312504/d776541d8k.htm (last visited Aug. 26, 2014); *see also Community Health Says Data Stolen in Cyber Attack from China*, http://www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818 (last visited Aug. 26, 2014).

7 *See id.*

8 *Id.*

Community Health Violated HIPAA and Industry Standard Data Protection Protocols

23. HIPAA was enacted and became effective in 1996.

24. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services create rules to streamline the standards for handling Sensitive Information, like the data collected and stored in unsecure database(s) by Community Health. The Department of Health and Human Services established standards to protect electronic personal health information from unauthorized disclosure. These standards require entities, such as Community Health, to adopt administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Sensitive Information.

25. Community Health's data breach resulted from a variety of failures to follow HIPAA guidelines and industry standards. Among such deficient practices, Community Health's breach shows that it failed to implement, or inadequately implemented, information security policies or procedures such as those requiring adequate encryption or similar protection of Sensitive Information. For instance, Community Health didn't implement adequate security protections designed to detect and remove security threats, such as the malware used to gain access to its

server here.[9] Worse still, Community Health didn't patch a widely-known vulnerability in its server's encryption software[10] despite the availability of such fixes.[11]

26. Community Heath's security failures demonstrate that it failed to honor its express and implied promises by failing to:

a. Maintain an adequate data security system to prevent data breaches;

b. Mitigate the risks of a data breach and unauthorized access to Sensitive Information;

c. Adequately encrypt or otherwise protect Plaintiff's and the

---

[9] *See Hospital Network Hacked, 4.5 Million Records Stolen*, http://fox59.com/2014/08/18/hospital-network-hacked-4-5-million-records-stolen/ (last visited Aug. 26, 2014).

[10] This vulnerability is commonly referred to as the "Heartbleed bug." In technical parlance, the Heartbleed bug is a "vulnerability in the popular OpenSSL cryptographic software library [*i.e.*, a server's encryption software] . . . This allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software . . . This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users." *The Heartbeed Bug*, http://heartbleed.com/ (last visited Aug. 26, 2014).

[11] *See Heartbleed Hack Still a Threat Six Months After Discovery*, http://www.bloomberg.com/news/2014-08-27/heartbleed-hack-still-a-threat-six-months-after-discovery.html (last visited Aug. 26, 2014); *see also* Heartbleed to Blame for Community Health Systems Breach, http://www.csoonline.com/article/2466726/data-protection/heartbleed-to-blame-

Class's Sensitive Information;

d. Ensure the confidentiality and integrity of electronic protected health information it created, received, maintained, and transmitted in violation of 45 CFR 164.306(a)(1);

e. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

f. Implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

g. Protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2);

h. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable

---

for-community-health-systems-breach.html (last visited Aug. 26, 2014).

health information in violation of 45 CFR 164.306(a)(3);

i. Ensure compliance with the HIPAA security standard rules by its workforce in violation of 45 CFR 164.306(a)(4); and

j. Effectively train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out their functions and to maintain security of protected health information in violation of 45 CFR 164.530(b).

27. Had Community Health implemented proper security protocols to properly encrypt and otherwise protect its patients' Sensitive Information, the consequences of the data breach would have been avoided (as it would have been nearly infeasible to extract its patients' data). Worse yet, Community Health knew or should have known that a security breach could result from its deficient security and privacy practices, as HIPAA and industry standard protections exist *specifically* to prevent unauthorized access to Sensitive Information and because fixes to the Heartbleed bug as well as the malware that infected its server were readily available.

28. Even though Community Health patients both expected and paid for the above-described security measures as part of their hospital experience (*i.e.*, that

HIPAA-mandated and industry standards would have been used to protect their Sensitive Information), they were not implemented, which resulted in the unsecured release of their Sensitive Information and the loss of paid-for data protection services.

Plaintiff Roman's Experience

29. Prior to July 2014, Plaintiff Roman had been a patient of Community Health's affiliated hospitals and clinics.

30. As part of the patient-admission process, Roman was required to provide Community Health with her Sensitive Information in exchange for an agreement with Community Health to receive health care services and to protect her Sensitive Information in accordance with HIPAA and industry standards.

31. As such, Roman paid Community Health for her medical care and, among other aspects of her treatment, the protection of her Sensitive Information.

32. Had Roman known of Community Health's substandard security procedures and methods of protecting and storing her Sensitive Information, she would have paid substantially less for Community Health's health care services or would not have paid at all (*i.e.*, the value of health care services *without* adequate protection of Sensitive Information is worth substantially less than the value of such services *with* adequate protection).

33. Because Community Health did not sufficiently protect her Sensitive Information, Roman did not receive the entirety of the services she paid for and, as a result, she paid more than she otherwise would have for such services.

34. Worse yet, Roman only learned that her Sensitive Information was compromised as a result of the breach after she learned about the breach and subsequently contacted Community Health herself.

CLASS ACTION ALLEGATIONS

35. **Class Definition**: Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(a), (b)(2) and (3) on behalf of herself and a class and subclass of similarly situated individuals, defined as follows:

> **Class**: All persons in the United States and its territories who (i) paid money to Community Health in exchange for health care related services, and (ii) whose Sensitive Information was compromised as a result of the data breach confirmed by Community Health in or around July 2014.
>
> **Pennsylvania Subclass**: All Class members who are residents of the Commonwealth of Pennsylvania.

Excluded from the Class and Pennsylvania Subclass (collectively referred to as the "Class," unless otherwise indicated) is (i) any judge presiding over this action and members of their families; (ii) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which Defendants or their parents have a controlling interest and their current or former employees, officers and directors;

(iii) persons who properly execute and file a timely request for exclusion from the Class; and (iv) the legal representatives, successors or assigns of any such excluded persons, as well as any individual who contributed to the unauthorized access of Community Health's patient records.

36. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but on information and belief, the Class is compromised of at least hundreds of thousands of individuals throughout the country, making joinder of each individual member impracticable. Ultimately, the members of the Class will be easily identified through Defendants' records.

37. **Commonality and Predominance**: Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting only individual members, and include, but are not limited to:

a. Whether Defendants took steps and measures to adequately safeguard Plaintiff's and the Class members' Sensitive Information;

b. Whether Defendants storing of Plaintiff's and the Class members' Sensitive Information in the manner alleged violated industry standards and/or HIPAA;

c. Whether Defendants' conduct described herein constitutes a

violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq.*;

d. Whether implied or express contracts existed between Defendants, on the one hand, and Plaintiff and the members of the Class on the other;

e. Whether Defendants' conduct described herein constitutes a breach of their contracts with Plaintiff and the Class members; and

f. Whether Defendants should retain the monies paid by Plaintiff and other Class members to protect their Sensitive Information.

38. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Class. Plaintiff and the Class sustained damages as a result of Defendants' uniform wrongful conduct during transactions with Plaintiff and the Class.

39. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiff.

40. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the members of the Class, and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply and affect members of the Class uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff or any other Class member.

41. **Superiority**: This class action is appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. The damages suffered by the individual members of the Class will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' wrongful conduct. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the

complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law
73 P.S. §§ 201-1, *et seq.*
(On Behalf of Plaintiff and the Pennsylvania Subclass)

42. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

43. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq*. ("UTPCPL") protects consumers from, among other things, unconscionable commercial practices, deception, fraud, false promises, false pretenses, and/or misrepresentations.

44. Community Health is a "person" as defined by Section 201-2(2) of the UTPCPL.

45. Community Health is/was engaged in "trade" and "commerce" as defined by Section 201-2(3) of the UTPCPL.

46. As described herein, Community Health has engaged in unlawful

and/or deceptive conduct.

47. Through its Notice of Privacy Practices, patient agreements, and security representations made on its websites, Community Health represented to Plaintiff and the Pennsylvania Subclass that it would, *inter alia*, protect their Sensitive Information, maintain the privacy of their Sensitive Information, follow the terms of the Notice of Privacy Practices in protecting their Sensitive Information, and comply with HIPAA and other federal and state law requirements.

48. Community Health's privacy and security promises were, in fact, false. Community Health did not maintain an adequate electronic security system to prevent data breaches, employ industry standard and commercially reasonable measures to protect its patients' Sensitive Information and mitigate the risks of any data breach or otherwise comply with the data security requirements of the HIPAA regulations, as promulgated under 45 CFR 164. Thus, Community Health's representations to Plaintiff and members of the Pennsylvania Subclass were false when made.

49. Knowing that consumers are less likely to do business with companies that fail to adequately protect their Sensitive Information, Community Health made the false privacy and security representations with the intention that Plaintiff and

the Pennsylvania Subclass members would rely on them in contracting with Community Health for medical services.

50. Because ordinary consumers lacked access to Community Health's proprietary information regarding its true privacy and security measures prior to the April and June 2014 breach, Community Health's false security and privacy representations were likely to deceive consumers who had no other resource for assessing Community Health's privacy and security practices.

51. Had Community Health disclosed its true security practices—which did not comply with state and federal law—Plaintiff and the Pennsylvania Subclass would have paid substantially less for Community Health's health care services or would not have paid at all (*i.e.*, the value of health care services *without* adequate protection of Sensitive Information is worth substantially less than the value of such services *with* adequate protection).

52. Community Health's deceptive and misleading actions were perpetuated while providing health care-related services to its patients, and therefore occurred during the course of its business practices.

53. Accordingly, and pursuant to 73 P.S. § 201-9.2(a), Plaintiff, on behalf of herself and the Pennsylvania Subclass, seeks: (i) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Pennsylvania Subclass;

(ii) actual damages or statutory damages of one hundred dollars ($100), whichever is greater; and (iii) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

54. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

55. Plaintiff and the Class members' paid money to Community Health in exchange for its promise to provide patient services.

56. In addition to providing medical care, a material part of Community Health's promise to provide patient services involved protecting Plaintiff's and the Class members' Sensitive Information.

57. In its written agreements as well as its patients' rights and privacy notices, Community Health expressly promised Plaintiff and members of the Class that Community Health only discloses health information when required to do so by federal or state law. Community Health further promised that it would protect their Sensitive Information.

58. Community Health promised to comply with all HIPAA standards and to make sure that Plaintiff's and the Class members' Sensitive Information was protected. Community Health further promised to provide notice to Plaintiff and

members of the Class describing Community Health's legal duties and privacy practices with respect to their Sensitive Information.

59. The contracts required Community Health to safeguard Plaintiff's and the Class members' Sensitive Information to prevent its disclosure and/or unauthorized access

60. Plaintiff and the Class members fully performed their obligations under the contracts.

61. Community Health did not adequately safeguard Plaintiff's and the Class members' protected Sensitive Information. Specifically, Community Health did not comply with its promise to comply with HIPAA's guidelines or industry standards when it stored its patients' Sensitive Information.

62. The failure to meet these promises and obligations constitutes an express breach of contract. In other words, Community Health breached the contracts with Plaintiff and the members of the Class by failing to implement sufficient security measures to protect Plaintiff's and the Class members' Sensitive Information as described herein.

63. Community Health's failure to fulfill its data security and management promises resulted in Plaintiff and the Class members receiving services that were of less value than they paid for (*i.e.*, the provision of medical

care without adequate data security and management practices).

64. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive—even though such protections were a material part of their contracts with Community Health—Plaintiff and the Class did not receive the full benefit of their bargain.

65. As a result of Community Health's breach, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Community Health's services as promised and the actual diminished value of its health care services.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(in the alternative to Breach of Express Contract)
(On Behalf of Plaintiff and the Class)

66. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 54-65.

67. In order to benefit from Community Health's services, Plaintiff and the Class disclosed Sensitive Information to Community Health, including their names, addresses, telephone numbers, Social Security numbers, dates of birth, and extremely sensitive medical diagnosis information.

68. By providing that Sensitive Information, and upon Community Health's acceptance of such information, Plaintiff and the Class, on the one hand,

and Community Health, on the other hand, entered into implied contracts whereby Community Health was obligated to take reasonable steps to secure and safeguard that information.

69. Under the implied contract, Community Health was further obligated to provide Plaintiff and the Class with prompt and sufficient notice of any and all unauthorized access and/or theft of their Sensitive Information.

70. Without such implied contracts, Plaintiff and the Class would not have provided their personal information to Community Health.

71. As described herein, Community Health did not take reasonable steps to safeguard Plaintiff's and the Class members' Sensitive Information.

72. Because Community Health allowed unauthorized access to Plaintiff's and the Class members' Sensitive Information and failed to take reasonable steps to safeguard their Sensitive Information, Community Health breached its implied contracts with Plaintiff and the Class.

73. The failure to meet these promises and obligations constitutes a breach of contract. In other words, Community Health breached the contracts by failing to implement sufficient security measures to protect Plaintiff's and the Class members' Sensitive Information as described herein.

74. Community Health's failure to fulfill its data security and

management promises resulted in Plaintiff and the Class receiving services that were of less value than they paid for (*i.e.*, the provision of medical care without adequate data security and management practices).

75. Stated otherwise, because Plaintiff and the Class paid for privacy protections that they did not receive—even though such protections were a material part of their contracts with Community Health—Plaintiff and the Class did not receive the full benefit of their bargain.

76. As a result of Community Health's breach, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Community Health's services as promised and the actual diminished value of its health care services.

FOURTH CAUSE OF ACTION
Restitution/Unjust Enrichment
(in the alternative to Counts II and III)
(On Behalf of Plaintiff and the Class)

77. Plaintiff incorporates the foregoing allegations as if fully set forth herein, excluding paragraphs 54-76.

78. If the Court finds Plaintiff's and the Class members' contracts with Community Health for protection of their Sensitive Information invalid, non-existent, or otherwise unenforceable, Plaintiff and the Class may be left without any adequate remedy at law.

79. Plaintiff and members of the Class conferred a monetary benefit on Community Health in the form of fees paid for health care services. Community Health appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class.

80. The fees for health services that Plaintiff and the Class paid to Community Health were supposed to be used by Community Health, in part, to pay for the administrative costs of data management and security.

81. Under principles of equity and good conscience, Community Health should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Community Health failed to implement data management and security measures that Plaintiff and the Class paid for and are otherwise mandated by HIPAA and industry standards.

82. Accordingly, as a result of Community Health's conduct, Plaintiff and the Class suffered damages in the amount of the difference between the price they paid for Community Health's services as promised and the actual diminished value of the health care services received.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Roman, individually and on behalf of the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class and Pennsylvania Subclass defined above, and appointing Plaintiff as representative of the Class and Pennsylvania Subclass, and appointing her counsel as Class Counsel;

B. Declaring that Community Health's actions, as described above, constitute (i) violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq.*, (ii) Breach of Express Contract, (iii) Breach of Implied Contract (in the alternative to Breach of Express Contract), and (iv) Unjust Enrichment (in the alternative to Breach of Express Contract and Breach of Implied Contract);

C. Awarding injunctive and other equitable relief as is necessary to protect the interests of the Class, including: (i) an order prohibiting Community Health from engaging in the wrongful and unlawful acts described herein, and (ii) requiring Community Health to protect all data collected through the course of its business in accordance with HIPAA and industry standards;

D. Awarding damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding restitution to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding Plaintiff and the Class their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiff and the Class pre and post-judgment interest to the maximum extent allowable by law; and

H. Awarding such other and further legal or equitable relief as equity and justice may require.

JURY DEMAND

Plaintiff requests trial by jury of all claims that can be so tried.

Respectfully submitted,

CAROSELLI BEACHLER MCTIERNAN & CONBOY, LLC

Dated: August 29, 2014

By: /s/ William R. Caroselli

WILLIAM R. CAROSELLI (PA 452)
WCAROSELLI@CBMCLAW.COM
20 STANWIX STREET, 7TH FLOOR
PITTSBURGH, PA 15222
TEL: (412) 391-9861
FAX: (412) 391-7453

DAVID S. SENOFF (PA 65278)
DSENOFF@CBMCLAW.COM
CAROSELLI, BEACHLER,
MCTIERNAN & CONBOY LLC
1845 WALNUT STREET, FIFTEENTH FLOOR
PHILADELPHIA, PENNSYLVANIA 19103
TEL: 215.609.1350
FAX: 215.609.1351

RAFEY S. BALABANIAN (IL 6285687)*
RBALABANIAN@EDELSON.COM
ARI J. SCHARG (IL 6297536)*
ASCHARG@EDELSON.COM
JOHN C. OCHOA (IL 6302680)*

JOCHOA@EDELSON.COM
DAVID I. MINDELL (IL 6309708)*
DMINDELL@EDELSON.COM
EDELSON PC
350 NORTH LASALLE STREET, SUITE 1300
CHICAGO, ILLINOIS 60654
TEL: 312.589.6370
FAX: 312.589.6378

**PRO HAC VICE* ADMISSION TO BE SOUGHT.

ATTORNEYS FOR SUSAN ROMAN,
INDIVIDUALLY AND ON BEHALF OF ALL
OTHERS SIMILARLY SITUATED